

This Page Is Inserted by IFW Operations
and is not a part of the Official Record

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

IMAGES ARE BEST AVAILABLE COPY.

**As rescanning documents *will not* correct images,
please do not report the images to the
Image Problems Mailbox.**



PATENT ABSTRACTS OF JAPAN

(11) Publication number: **10143493 A**(43) Date of publication of application: **29 . 05 . 98**

(51) Int. Cl. **G06F 17/10**
G09C 1/00
H03M 7/50

(21) Application number: **08336202**(22) Date of filing: **13 . 11 . 96**(71) Applicant: **SEIBU:KK**(72) Inventor: **SHONO KATSUFUSA**
AKIYAMA MUNEYUKI(54) **TIME SERIES FOR CHAOS**

(57) Abstract:

PROBLEM TO BE SOLVED: To make chaos industrially practicable by matching a square quantum size by nonlinearly performing quantization processing to a nonlinear function.

SOLUTION: At the time of nonlinearly quantizing the linearly quantized time series of the internal state of the chaos again, inclination is obtained for all input corresponding to the quantum of an equal size on the input/output transmission characteristics of linear quantization, classification is performed corresponding

to the inclination, re-classification is performed by a threshold value processing based on defined weight, normalization is performed, bundling is newly performed and the quantization is performed. By taking out the square quantum of the matched quantum size without overlap on the graph of the transmission characteristics along a 45 degree line, allocating a blocked digital code and attaining an input code, a cipher restoration system utilizing the chaos is made designable. The allocation of the input code without the localization of distribution is made possible and the internal state of the chaos is effectively utilized.

COPYRIGHT: (C)1998,JPO

(19) 日本国特許庁 (J P)

(12) 公 開 特 許 公 報 (A)

(11) 特許出願公開番号

特開平10-143493

(43) 公開日 平成10年(1998) 5月29日

(51) Int.Cl.⁶

識別記号

F I

G 0 6 F 17/10

G 0 6 F 15/31

Z

G 0 9 C 1/00

6 1 0

G 0 9 C 1/00

6 1 0 Z

H 0 3 M 7/50

H 0 3 M 7/50

審査請求 未請求 請求項の数1 書面 (全 4 頁)

(21) 出願番号

特願平8-336202

(22) 出願日

平成8年(1996)11月13日

(71) 出願人 596180995

株式会社セイブ

佐賀県西松浦郡有田町西部甲753

(72) 発明者 庄野 克房

神奈川県横浜市旭区白根5丁目45番12号

(72) 発明者 秋山 宗志

佐賀県西松浦郡有田町中樽3丁目5番15号

(54) 【発明の名称】 カオスのタイムシリーズ

(57) 【要約】

【目的】 非線形一次写像回路の生成するカオスのタイムシリーズを非線形に束ねなおして量子化し、伝達特性の中に見出される1対多又は多対1の関係を産業に利用する。

【構成】 線形に量子化して計測したカオスのタイムシリーズの入出力伝達特性上で傾斜を求め、傾斜に応じた重みで非対象に束ねなおすことにより非線形に量子化しなおしたタイムシリーズを用い、デジタルデータの検索を行い過去に戻った複数の状態への変換とその逆変換を利用する電子情報通信分野におけるデジタル情報処理技術である。

【特許請求の範囲】

【請求項1】 線形に量子化したカオスの内部状態のタイムシリーズを非線形に量子化しなおすにあたって、線形量子化の入出力伝達特性上において等しいサイズの量子に対応する全ての入力について傾斜を求め、傾斜に応じた分類をし、定義された重みにもとづくしきい値処理により再分類をするとともに正規化をしてあらためて束ねなおし量子化したことを特徴とするカオスのタイムシリーズ。

【発明の詳細な説明】

【0001】

【産業上の利用分野】本発明はカオス発生回路が生成するカオスの内部状態 $y(t)$ (t は離散時間、 $t = 0, 1, 2, \dots$) の作るタイムシリーズ $y(t) - t$ の量子化手法に関する。

【0002】従来のエレクトロニクス産業は1対1対応関係のもとで明確な因果関係にのみしたがって構築されてきた。一方、非線形次元写像回路の生成するカオスには、その過去には分岐を生じ、将来には発散と収束を*

ビット汎用ADCで線形に量子化した内部状態を $y_{16}(t)$ と書くと、 $0 \leq y_{16}(t) \leq 65563$ である。電子回路の合成関数が与える次元写像関数次元写像関数 f により生成されるカオスの伝達特性は

$$y_{16}(t+1) = f\{y_{16}(t)\} \quad (1)$$

により入力 $y_{16}(t)$ と出力 $y_{16}(t+1)$ の関係として与えられる。

【0007】カオスのタイムシリーズ $y_{16}(t) - t$ を離散時間 t に沿って検索し、 $y_{16}(t)$ を発見したら τ ステップ過去に戻った値 $y_{16}(t-\tau)$ 、あるいは τ ステップ将来の値 $y_{16}(t+\tau)$ も求めることができ、入力 $y_{16}(t)$ に対する出力 $y_{16}(t-\tau)$ あるいは $y_{16}(t+\tau)$ の関係が求められる。

【0008】カオスの過去には分岐を生ずるので、 $y_{16}(t-\tau)$ は複数の異なる整数値となる。将来には決定論的に状態が決まるが発散と収束を繰り返すので、 $y_{16}(t-\tau)$ は整数値の幅を持った値となる。

【0009】 $y_{16}(t)$ から出発し過去へ τ ステップ戻り、再び τ ステップ将来へ進んだ値を $y_{16}(t-\tau+\tau)$ と記すと、 $y_{16}(t)$ と $y_{16}(t-\tau+\tau)$ は往復した伝達特性となる。 $y_{16}(t)$ を横軸にとり $y_{16}(t-\tau+\tau)$ を縦軸にとったグラフは、45度線に沿って正方形が並ぶことになる。非線形関数 f の伝達特性を線形に量子化して計測したとき、量子サイズが様々となり、往復した伝達特性の正方形のサイズは様々で相互に重なり合う。

※

$$w'\{y_{16}(t)\} = \frac{w\{y_{16}(t)\}}{\sum_{y_{16}(t)=0}^{65563} w\{y_{16}(t)\}}$$

【0015】次の式を満足するように8ビット非線形量

*繰り返す。1対多及び多対1の対応関係を内蔵し、新しい産業の可能性を与える。

【0003】1対多の関係は暗号コードの生成に、多対1の関係は暗号コードの復元に利用される。

【0004】多対1の関係は画像や音声データの圧縮に利用され、1対多の関係を利用して再生展開される。

【0005】

【従来の技術】増加関数を与える電子回路と減少関数を与える電子回路の入力および出力を共通にした並列接続により関数合成を行う次元写像回路を、CMOSスイッチを介してフリップフロップのループに構成することにより、カオス発生回路が実現される。そのとき、カオス発生回路の入出力伝達特性が解析的な関数関係で記述できるわけではない。

【0006】分解能16ビットのADC（アナログ・デジタル変換器）でカオス発生回路の内部状態 $y(t)$ を計測したとする。 $y(t)$ は0～65563の量子（整数）のいずれかに属する。初期値 $y(0)$ は0～65563の量子の一つである整数で与えられる。16

※【0010】カオスの応用、たとえば暗号化復元システムを設計するとき、量子サイズが不揃いだと、カオスの内部状態を平等に有効利用することが難しい。本発明は、非線形関数を非線形に量子化処理を行うことにより、正方形の量子サイズをそろえ、カオスの工業的実用化に道を開くものである。

【0011】

【課題を解決するための手段】線形に計測したタイムシリーズ、たとえば $y_{16}(t) - t$ を非線形に束ねなおすことにより量子サイズをそろえる処理のアルゴリズムは以下の通りである。関数 f は計測はされるが、解析的に関数関係で記述できないので、非線形処理は数値的に行われる。

【0012】すべての $y_{16}(t)$ に関し、傾斜 $df/dy_{16}(t)$ を求める。

【0013】 $df/dy_{16}(t)$ が、たとえば2より大きい $y_{16}(t)$ には重みとして $w=1.5$ を与え、 $df/dy_{16}(t)$ が2より小さい $y_{16}(t)$ には重みとして $w=1.0$ を与える。すなわち傾斜2をしきい値として、2以上の傾斜を緩くするように重みを与える。

【0014】16ビット線形量子化の内部状態 $y_{16}(t)$ を8ビット非線形量子化の内部状態 $y'(t)$ に束ねなおす場合を考える。次式にしたがって正規化した重み $w'\{y_{16}(t)\}$ を求める。

$$(2)$$

子化の境界 $B(q)$ をもとめる。

$$\sum_{y_{16}(t)=0}^{B(q)} w' \{y_{16}(t)\} = \frac{q+1}{2^8}$$

ここで q は0, 1, 2, ..., 255であり、 $B(255) = 65563$ である。

【0016】以上の非線形区分を、線形16ビットから非線形8ビットに変換した例に限らず、一般化すること*

タイムシリーズを離散時間 t に沿って検索することにより、発見された $y'_8(t)$ に対し τ ステップ過去に戻った内部状態の値 $y'_8(t-\tau)$ は複数個存在する。理想的には 2^{τ} 個発見される。 $y'_8(t)$ を入力コードとするとき、複数個発見される $y'_8(t-\tau)$ は暗号コードとするのにふさわしい。複数個のうちどれが現れるかは確率によって決まり、予測することは難しい。 ※ ※ 【0019】

離散時間 t を検索し、暗号コード $y'_8(t-\tau)$ を発見したら τ ステップ将来へ進み $y'_8(t-\tau+\tau)$ を見出すことができる。 $y'_8(t-\tau+\tau)$ は、入力コード $y'_8(t)$ を含むが、

発散のためにある幅を持って広がっている。その広がり
は、理想的には 2^{τ} ビットである。

【0020】

20

$y'_8(t)$ から $y'_8(t-\tau+\tau)$ を見たときの往復した伝達特性上では、45度線上に、

理想的には 2^{τ} ビット巾の正方形が $2^{8-\tau}$ 個等間隔に配置される。たとえば、 $\tau=4$ とすると $2^4=16$ ビット巾の正方形の量子が16個配置される。

【0021】

【実施例】通信線を介して電送されるデジタルコード列を暗号化復元するシステムについて実施例を述べる。

【0022】16個の正方形には、文字、画像、音声などの4ビットデジタルコード16個を対応させて割り当てる。この割り当ての組み合わせは有効な暗号鍵である。その組み合わせの種類は $16! = 2.09 \times 10^{13}$ ★

タイムシリーズ $y'_8(t)-t$ 上で暗号化復元を行った場合、ペンティアム 133 MHz CPU及び32Mバイトメモリを用いたとき、暗号化処理速度11.6kバイト/秒、また復元処理速度16.7kバイト/秒が達成された。

【0025】暗号化処理は任意の離散時間 t からの検索☆

より高速な暗号化を実現するためには、タイムシリーズ $y'_8(t)-t$ を、離散時間 t を残してハッシュテーブル化することである。この手法を採用することにより、4ビット単位にブロック化したとき最高2Mバイト/秒の暗号化処理速度が実現できた。8ビット量子化のタイムシリーズで $\tau=4$ と選んだ本実施例は理解しやすい1例にすぎない。16ビット量子化のタイムシリーズで $\tau=8$ とし8ビット単位でブロック化するなど、実際の工業的利用にあたっては一般化して実施されることは当然である。

【0027】暗号化復元は1対多から多対1への変換を利用した実施例であるが、多対1対応をデータ圧縮過程に利用し、1対多対応を圧縮データの展開再生に利用して画像や音声データの圧縮転送を実現することができ

*は容易である。また、上記の非線形区分処理を複数回繰り返しても効果がある。

【0017】

【作用】分解能8ビットに非線形量子化し、量子サイズをそろえたタイムシリーズ $y'_8(t)-t$ の中には1対多または多対1の伝達特性が見出される。

【0018】

★¹³通りである。十分使い捨て可能な数の暗号鍵が用意できる。

【0023】 τ を大きく選ぶと、暗号コードの種類は増えるが、定義できる入力コードの数は減少する。 τ を小さく選ぶと、暗号コードの種類は減るが、定義できる入力コードの数は増大し、暗号鍵の組み合わせの数は指数関数的に増大する。

【0024】文字、画像、音声などのデジタルコードを4ビット単位にブロック化し

☆を保証する必要があるが、復元処理ではタイムシリーズをテーブル化して処理速度の高速化を計ることができる。

【0026】

【0028】

【発明の効果】以上、実施例を用いて詳しく説明したように、一次元写像を用いたカオスの内部状態を、たとえば汎用ADCで線形に計測して一連のタイムシリーズ $y'_8(t)-t$ を求め、量子サイズをそろえるように束ねなおす数値処理のアルゴリズムが具体的に示された。タイムシリーズ上で往復した伝達特性 $y'_8(t)-y'_8(t-\tau+\tau)$ のグラフ上で、量子サイズのそろった重なりのない正方形の量子が45度ラインに沿って取り出され、ブロック化したデジタルコードを割り当てて入力コードとすることにより、カオスを利用した暗号化復元システ

ムが設計可能となる。分布にかたよりのない入力コード
の割り当てが可能となり、カオスの内部状態を有効利用 *

* できるようになった。本発明の電子情報通信産業におけ
る情報の安全管理に寄与する効果は顕著である。